ELECTRICAL SYSTEMS: SECURITY

INTRODUCTION

The security system needs of public buildings, especially those considered "high profile", have increased dramatically in the last few years. With the attack on the Federal Building in Oklahoma City, enhanced security measures have become a high priority with a renewed commitment to the safety of the people. Buildings that become targets are selected because of several reasons, with symbolism and rage being among the highest on the list. The Capitol certainly is the symbol of the State of Utah. This was indicated in a recent survey, conducted by Mr. Greg Rollins of the Federal Protective Service in Salt Lake City, of the existing physical security at the State Capitol and the surrounding buildings. This report has been reprinted and placed in the Appendix for reference.

With the intent of restoring the building historically comes the challenge of integrating a higher level of security into the facility without impacting adversely the intent of returning to the original designs. These challenges can be met with a greater understanding of the intent of security and the role it will play in the safety of the Capitol and the people that visit. The technologies of security have been steadily advancing and do present some alternatives to some of the pre-conceived ideas of barred windows, heavy locks and obtrusive cameras. However, by the same token, society has become accustomed to the need for security check stations at the airports and other federal and justice buildings. The challenge for good security lies somewhere in between.

The intent of this report is to analyze the current security, both hardware and implementation, as well as explore the future possibilities that will enhance the safety of the building with measures that will meet the expectations that many people have now for their public buildings.

The standards and criteria are developed to address the project goals of:

Life Safety

Function - Efficient / Effectiveness

Historic / Architectural Integrity

1. LIFE SAFETY

a. STANDARD: Prevention of security concerns

1)Objective: Implement security systems, and procedures which deter unlawful behavior.

b. STANDARD: Reliable prevention, detection, and alarm response systems

1)Objective: Implement state of the art security electronics with redundant systems.

2. FUNCTION - EFFICIENCY / EFFECTIVENESS

a. STANDARD: Minimize the impact of security systems and procedures on the general public and building occupants.

1) Objective: Implement minimally intrusive security barriers, detectors, and personnel at both interior and exterior locations

3. HISTORICAL / ARCHITECTURAL INTEGRITY

a. STANDARD: Mandate the extremely high quality installation of security systems, thereby preserving the historical and architectural integrity of the capitol.

1) Objective: Employ craftsmen who understand the magnitude of the capitol restoration, and who have demonstrated the ability to complete their work in full compliance with the highest standards of acknowledged industry practices, and all installation practices identified in the Uniform Building Code, and Sound System Engineering, (2nd Edition), D. Davis.

4. MINIMUM QUALITY LEVELS AND MANDATORY STANDARDS:

a. NFPA 70, "National Electrical Code."

b.UL Standard 609, 1023, and 1076

c. Electrical Code Compliance: Comply with applicable local code requirements of the authority having jurisdiction and NEC 800-Series articles as applicable to installation, and construction of video surveillance equipment and signal distribution systems.

d..UL Compliance: Comply with applicable requirements of UL Standards 486A and B, 813, 983, 1409, 1410, 1412, 1414, 1416, 1417, and 1418 pertaining to video surveillance system products. Provide video surveillance systems and components which are UL-listed and labeled.

e. IEEE Compliance: Comply with applicable requirements of IEEE 208, "Video Techniques: Measurement of Resolution of Camera Systems."

f. EIA Compliance: Comply with applicable requirements of Electronic Industries Association Standards RS-170, 222, 232, 312, 330, 403, 412, 420, 439, and 455 pertaining to video surveillance equipment and accessories.

g. FCC Compliance: Comply with Subpart J of PART 15, FCC Rules pertaining to computing devices including Class A, Class B, personal and peripheral types. Provide equipment which complies with technical standards for both radiated and power line conducted interference.

The electronic security systems presently employed at the Capitol Building include video surveillance, card access/intrusion detection, and limited duress annunciation. Building occupants rely principally upon security personnel, particularly during peak periods of use, and less upon electronic security systems.

Video Surveillance: Surveillance cameras are located sporadically throughout general public thoroughfares, and in sensitive building offices and rooms. Cameras are generally fixed position, analog, color, and NTSC with approximately 450 lines of resolution.

All camera signals converge at the security control room. At this location, multiple video monitors are used to view camera signals. Video switchers are under the control of the monitoring personnel, who can select the desired camera signals for display.

The conclusions reached in this report are based on some objectives and guidelines that guide the discussion of current security conditions in the various facilities on the Capitol campus. Security is to provide peace and protection and safety from outside influences. There are essentially three main parts to any attempt to secure these places and things from these outside influences, and they are:

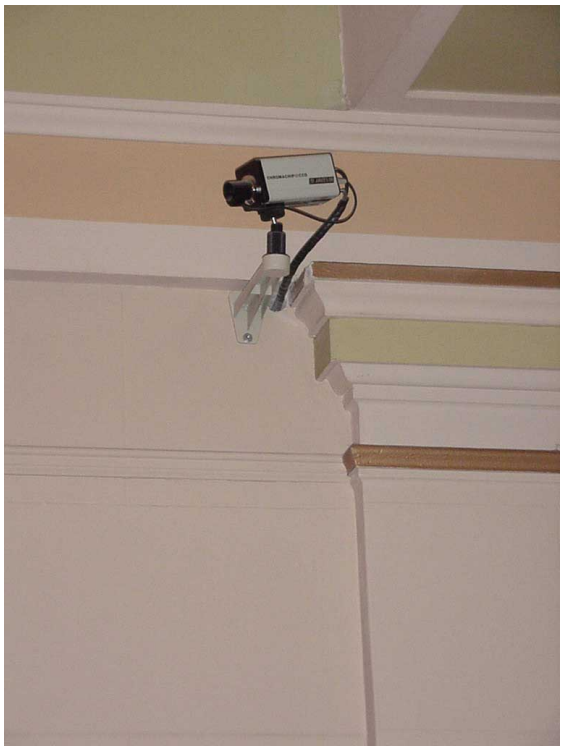
Prevention.

Detection.

Alarm Response.

1.Prevention

a. If done well, prevention can eliminate a major portion of security concerns before they start. The purpose of prevention is to discourage people from doing something unauthorized or unacceptable. This is usually done on the exterior of a building by making any restricted entrance more difficult to access or physically undesirable. Physical barriers, locks, gates, and controls are all customary. It is also respectful to redirect those desiring to use a non-public entrance to the location where they can enter by the use of signs. Access control and monitoring of service and staff entrances can eliminate most of the unauthorized traffic in the buildings. This can be done without creating a "Fort Knox" appearance, but at the same time, provide security officers total control of the entries to the building. The use of visible cameras in these restricted areas increases the effectiveness of the security.



EXISTING CAMERA INSTALLATION

b. Prevention inside a public building becomes less simple. The presence of X-ray machines and metal detectors really destroys the "open" feeling of the building. The desires to maintain the areas listed by the architect as Preservation Zone 1 and also to reverse the trends in the areas listed as Impact Zones and return them to a Zone 1 level, discourage dramatically this level of prevention inside the building. Perhaps, as was indicated in the Physical Security Study done by Mr. Rollins, some type of reception desk could be implemented. It could appear as having more of an "information" feel to it, while at the same time providing a security check point. This desk would be advisable for sure in the other buildings that comprise the Capitol campus, since they are more employee and staff oriented and less public intensive.

c. The proliferation of cameras inside the Preservation Zone 1 areas of the Capitol should also be kept to a minimum. With the advent of discreet dome cameras, typically 5 to 7 inches in diameter, these large entry spaces can be viewed well without impacting walls that previously held mounts and camera enclosures. The intent of the cameras at encouraging good behavior could be enhanced by a simple, concise, unobtrusive sign indicating the presence of video surveillance. For some people this is negative, but for far more people, it contributes to a higher feeling of safety.

d. All non public doors should be access controlled with card readers or kept locked. Security officers should not be tasked with constantly monitoring all exit doors; only when the door remains unsecure should they be notified. This will lessen some of their sometimes overwhelming burden. Currently, many of the these types of doors on the campus are being propped open, left unrepaired and therefore do not close well, or are just not monitored at all with either camera or door contact indicator switches. Delivery dock doors were left open with easy access to anyone. Controlled access can prevent most unfortunate occurrences and should be implemented on all non public doors, with check in and out procedures for all delivery dock areas. Refer again to the physical security survey prepared by Mr. Rollins.

e.In a general sense though, most preventative security measures are aimed at discouraging obvious and mischievous actions. Physical barriers, signs, and cameras will deter most people with no real intent to do harm. However, as society becomes more unruly, and the ability for people to repeat the circumstances in Oklahoma City become more real, almost anything is possible. The need for security to deal with this level of threat is not only necessary but required.

f. So as we look at the possible threats to the safety of the building and the people at large, the range goes from simple acts of vandalism and mischief to actual destruction and harm. Listed below are possible threats that the security system, officers and contingency plans will need to deal with.

1)Vandalism, nuisance acts, graffiti, etc.

2)Building intrusion, burglary, inside covert actions, etc.

3)Individual acts of violence, sniper, mugging, etc.

4 Hostage takeovers involving either individuals or groups.

5)Extensive and widespread destruction. (Oklahoma City)

g. What would follow the more serious of these threats is immediate public panic, much media coverage, and a public thirst for blame. These are the desired results for those with real intent. In most cases, they can not be prevented from carrying out their agenda, but by prior preparation and early warning detection, these types of serious threats can be dealt with quickly, and hopefully, the impact dramatically reduced. The last thing anyone wants to hear is, "Why couldn't we have done something to avoid this ?"

3. Detection

a. The intent here is to have in place an " early warning " system that will notify security officer's of immediate situations, rather than finding out about them hours later or even the next day. When cameras are used to monitor areas, the impression generally is that all things are being watched. This is just not true. Yes, the camera is watching, but the camera will not reach out and stop the misdeed. However, the person looking at the camera cannot know for sure that someone is watching or not, thereby providing the preventative deterrent. But for those watching a large number of monitors for very long, seeing all the potential dangers in not physically possible. Other means of detection should be used to direct the attention of the officers that watch.

b. Typically, these other means of detection include such devices as door contact indicator switches, motion detectors, beam detectors, high load detectors at vehicle entrances to the campus and delivery areas, and other hardware that indicate a presence of potential danger where there should not be any. By interfacing these subsequent indicators into a video system, these "alarms" could call up any associated cameras and the officer is now spending the time watching actual events and not just monitoring cameras looking at nothing. For instance, someone using an access card at the back door "activates" or switches the image from the camera looking at that door to the main screen in the security office. The officer's full attention is now on who is going through that door, or gate, or office area.

c. Another bit of technology greatly improves the camera's ability to focus the officer's attention. Motion detection equipment can now be placed between the camera and the monitor screen. When motion is detected in the area the camera is "watching", a similar alarm contact created by the motion detection equipment can be interfaced to the video system to call that camera's image to the main screen. An officer could sit all night watching twelve cameras that cover the grounds of the Capitol and could miss a lot of things. But if the camera and motion detection equipment alerts them to any motion, their attention would be immediately focused on that camera being displayed on that monitor.

d. There are areas where cameras are necessary for the monitoring of the building, but are not used as preventative measures. These cameras should not be seen. Inside offices,

reception areas, publicly restricted walkways, high priority spaces such as security offices, emergency operations centers, etc., or any place where security needs to be monitored, cameras can be mounted almost anywhere. With the advent and increased refinement of "chip" cameras, the relative size is very adaptable to any type of installation. They can hide in pictures, in clocks, in smoke detectors, in motion detectors. Special attention will be needed to adapt the security cameras to the various preservation zones and impact areas so that their usefulness is enhanced, but their presence is unnoticed. Cameras being placed inside ornate wood carving displayed as part of the walls of the newly restored Capitol building in Ohio is an example of this adaptability.

e. The video cameras can be either fixed in place, always looking at the same view, or have pan/tilt/zoom capability. With this ability a single camera can cover a lot of ground. However, the drawback is that it requires someone to operate it. If the officer is constantly moving this one camera around, he is not paying much attention to any of the others. The pan/tilt/zoom cameras, or PTZ cameras, do come with software that allows a "tour" of motions to be preprogrammed into the controls and once activated the camera will move through these same motions repeatedly. But again, the power of the camera is only as strong as the attention given to it. If there are very many of these PTZ's running, a lot could be missed. The other theory is that there is no real problem with this because everything is being recorded anyway. That assumption however destroys the "early warning" concept. The officer needs to know now what is going on, not watch what happened on tape a few days late.

f. Recording video surveillance images typically is done on tape using time lapse recorders. Now there is another option, digital recording. Here the information is recorded digitally onto a hard drive and later saved or "archived" to a CD. Digital recording, although it is more expensive, does allow immediate access to any day, any time and any camera's image. Any one who has fooled with tape to try and find a particular time and day will totally appreciate this advantage.

g. The access control system would monitor all doors, gates, etc. with card readers. The Capitol currently uses an access control system on a majority of the exterior doors and some interior doors. For the system to be really useful, the cards issued to the employees should also include video badging, or the inclusion of their picture not only on the card but also in the database. When someone presents their card to the reader the security system could then not only identify by name who is using the card, but also by a video image seen in the central station.

h. Another system that has immense utility is the advent of wireless duress systems and their ability to triangulate, or sense exact location based on the received strength at different

antenna locations. Rather than hard wiring duress switches from public counters, chambers, offices, and such, an arrangement of antennas is installed above the ceilings throughout the building. This allows for portable transmitters to be carried on the person or fixed transmitters to be located at the usual counters and such. A press of the button and the location is immediately seen at the central security station. It will even track movement if the transmitter moves following the activation of an alarm.

i. The intent of the central security monitoring station should be a movement toward less monitors to watch at the same time, less dings, rings, buzzes, and tones to pay attention to and have the various systems all integrated into one security software package. The intrusion detection part of the system would monitor the door contact switches, the motion detectors, and the glass break indicators. The access control system monitors the status of all the doors with readers as well as the card holders. The video system would collect all the camera feeds, provide the officer with the ability to view any camera on any screen at any time by using the "matrix" switch part of the system, and send all camera feeds to the recording section of the system. The duress system would immediately show the location of the person activating the duress alarm and who it is assigned.

j. The real advantage of an integrated system is to have all these different parts seen at the same time on a single computer terminal. The view would be a floor plan indicating all access doors, locked doors with contact switches, all motion detectors and all camera locations. Any door opens, the indicator flashes and tones. If a camera is associated with that door it is seen immediately on the video system's main monitor. Someone uses their card to access a door, their picture, name and other info is shown on the screen. By touching any device or camera on the screen calls that camera up or gives you a recent history of the events for that device. A one man show. This allows other officers to be visually present in public, free to check out alarms or disturbances, escort money, check deliveries, etc. The number of video system monitors can be reduced requiring less real estate for the central station, and less fatigue factor on the officers. This is because they are spending their time focusing on events not empty camera images.

k. Granted, this could sound like the security systems are becoming more sophisticated and less "user friendly". Actually the opposite is true. By letting the machinery do the detecting of motion, or door openings, duress locations, or other intrusions and then bringing the actual events to the officer's attention, the monitoring of all the devices and cameras is less fatiguing and the officer is able to stay on top things better. The real secret to a successful detection phase of any security plan is to make it as painless as possible to the officers, while maintaining a high level of security. If it is too cumbersome, inconvenient, or difficult to deal with, human nature will kick in and the system will either be underutilized or

ignored. The remote detection devices are only as good as those who monitor the warning signal and deal with the alarm at the time.

4. Alarm Response

The third part of a successful security plan deals with the response to the detection devices' alarms. This can be the most effective part of the plan if pursued with intent and fidelity to the overall objectives. Circumstances that are dealt with quickly can also be dismissed quickly, once resolved. The largest detriment to this part of any plan is the lack of prior procedure and policy definitions, actual response preparation and follow through. When there is confusion about what to do next when an alarm comes in, the security plan's real effectiveness disappears very quickly. This confusion will increase the probability that the security measures once thought very important will become in time less used and more ineffective when really needed.

There are many different ways in which this prior preparation can be implemented. The following are some suggestions of processes and procedures that could be implemented.

a. Simple procedures that would involve the day-to-day alarm responses such as radio contact with field personnel in the area to go by and check things out. This immediate response on the part of the security team is the key to "de-fusing' a situation before it escalates. It requires "ready" personnel to respond quickly which is typically deterred by the fact that individual security team members are tasked with too many other responsibilities. By allowing the electronic hardware part of the system to handle most of the detection, personnel are freed up to respond.

b. Different levels of attention or response could be implemented that would deal with threats that are more serious. This would be similar to the military's DEFCON system that ranks supposed circumstances and calls into play different procedures. For instance, detection in higher priority areas could be "programmed" into the system to produce a different alert tone or message that would bring into play a different set of procedures on the part of the personnel. By identifying the most crucial points in the protection process, these alternative procedures are more effective during the more serious threats.

c. Worst case scenarios could be worked through before they actually happen and courses of action outlined with specific responsibilities defined prior to an actual event. This will greatly contribute to a higher comfort level when security officers and administrators are faced with some ugly possibilities and disasters.

d. Once these prior preparation responses are defined, a regular process of training and drills will help the "follow through" part of alarm response and will complement the entire security system plan and provide a higher level of comfort. When things become more of a habit, they become less inconvenient and more likely to happen when they really need to.

Security is not a take it or leave it proposition anymore, however, there are some areas wherein a bit a latitude in the implementation could be considered. Some particular areas involve how extensive the preventative measures provided outside and inside the buildings will be considering the desire to keep the Capitol a great place to visit. Too much visible security can detract, while too little provides no real protection. Other alternatives involve the economics of existing systems versus new technology.

1. From a security perspective, the more physical barriers like fences and gates that are used, the better. Also, the recommendation found in Mr. Rollins' survey to remove all the pine trees and reduce all other trees to seven feet or less is not a likely choice by any architect. By selectively placing fences and gates in "behind the scenes" areas such as delivery and maintenance locations, the public will not notice them as restrictions, but rather as prudent measures. The security objective is that no undetected approach to the building and grounds should be possible. Progress into publicly restricted areas needs to be impeded to allow security the time to check and monitor any approach events. This can be done well, but with more inconvenience than is present at the facilities today. Coming and going presently is far too unmonitored. Refer again to the survey reprinted in the Appendix. There should also be no question that all entrances into the buildings should be monitored.

2. Coordination between prospective camera angles and landscaping should be a compromising solution wherein the two compliment each other. By aligning trees, shrubbery, sidewalks, and open areas with the camera coverage, both could coexist well.

3. Preventative measures installed inside the building should be a combination of alternatives. In direct public view, the use of detection machines (Metal and X-ray detection) should be discouraged. But as progress continues into more restricted areas of less direct public view, such as offices, chambers areas and the main galleries where direct interaction with people is anticipated, these measures should be expected.

POTENTIAL LOCATION FOR METAL DETECTORS AND X-RAY

Other possible solutions to the prevention of unimpeded progress into higher priority areas is the use of glass walls and half walls in reception and office areas. This provides a physical barrier but retains at the same time an open "feel" to the space. The glass also makes a great background for etched seals and logos.

EXISTING MOTION DETECTOR

4. The alternatives for the public open areas are the more subtle forms of deterrence like visible but discreet cameras, simple informative signs, possible "Information" desks, and the constant presence of security officers. The monitoring effort should be a combination of these alternatives, not just relying on one of them to be enough.

5. "Littering" the inside of buildings with door switches, motion detectors and such has never been very acceptable to architects or interior designers. The security industry has addressed this by reducing the size of these devices and have also made them less obtrusive in shape and contour. They can be made to look like track lights for instance. For security, all exterior doors have door switches mounted inside the frames and all first floor areas with windows or similar access into the building from ground level or roof levels should have motion detectors to cover the space.

EXISTING SECURITY CONTROL CENTER

6. Wiring is always a concern, usually from the fact that security is sometimes an afterthought and the wiring is surface mounted in many cases. If the security system is designed as an integral part of the infrastructure and construction, this wiring problem goes away. There is also the ability to use wireless detectors is areas where direct wiring is not possible.

7. The central security monitoring location should be revisited. The alternatives involve staying with current implementation and save money by reusing equipment and

continue using the very "busy" atmosphere that currently exists, or, to simplify the operation with new equipment, integrating all facets of the security picture and reducing both the size of the area needed and the level of fatigue caused by having so many things to pay attention to. Of course the question is based in economics. Up front, the costs for new equipment are larger. But the life cycle costs which involve manpower, future upgrades and expansions, and better protection become less. This is because the open platforms used for the new technologies contribute to continued upgrade and expansion through modularity, rather than the "patch work quilt" method of adding more monitors and lights to an already large panorama of things to watch.

8. The access control system should be a complete and total system rather than a combination of different makes and models, card readers or keypads, proximity or card "swipe". Again, economics can be a factor because much of this equipment already exists in the buildings. However, from a control and maintenance perspective, a single database where all card holders are registered makes the most sense. It eliminates doors being opened with numbered codes or other types of cards and makes for a single point of authorization. More than one entity can not grant authorization. The issuance of only one type of card keeps everyone on the same page.

9. Duress systems have always been a hard wired proposition. Switches were installed at locations of possible duress such as cashiering or high profile offices (judges, for instance). The expectation of the system was that the person under duress would always be in reach of the switch. In other words, the liability of the duress system was the placement of the switch. The new technologies providing for wireless communication puts the switch in the hands of those responsible wherever they might be. And permanently mounted switches are still available, only without the wires. This would be an addition to the systems currently at the Capitol and would supplement the radio communications shared by the security officers.

10.Emergency call stations at parking lot and grounds locations provide for manual alarm notifications. Call stations can provide for different functions, which include video, audio, and duress annunciation. All stations should be placed as to be seen well by at least one of the perimeter cameras. This will eliminate the need for a separate camera in the station itself. Audio and a duress button are essential for a person to manually activate an alarm. The audio function provides "ears" to the security officers and the duress button initiates the whole process. The button not only opens the audio channel, but triggers any programmed cameras to immediately locate and zoom-in on to the station. Within seconds the officer is seeing and hearing the situation. These stations need to be very visibly marked to provide both deterrence and public awareness of their presence.

1. The overall existing security system has some separate systems with considerable need for improvement, and some desirable systems are not currently in use. It is recommended that all electronic aspects of the security system be implemented in such a manner as to allow fewer required security personnel to control the system from a singular computer based system. The equipment and monitoring functions will be located in a main security room. It has been found that even with the most sophisticated and powerful security system, without simple user interface and control, the system can be greatly limited. The human factor has been ignored in many cases.

2. It is recommended that the video system be seriously improved. All outside areas should be visible from a camera. This should be done through a combination of both fixed and controllable cameras. Fixed cameras should be focused on limited spaces such as docks, back door entrances, blind alleys, utility tunnels, service accesses, and blind landscaped areas. Pan/tilt/zoom cameras should cover the large open landscape areas and parking. These cameras should be programmed with "tours" of view which repeat continually. The "tour" can be interrupted at any time for manual viewing. Outside cameras should have high resolution, low light capability and protected environmentally. It should also be a high coordination priority to compliment camera coverage with proposed landscaping.

3. All public areas inside the Capitol should be visible from a camera. This again should be done through a combination of both fixed and controllable cameras. Fixed cameras should be focused on hidden spaces that can not be seen directly from the controllable cameras. There should be no less than two opposing pan/tilt/zoom cameras covering the inside large open area and providing two different views of any location. These cameras should be programmed with "tours" of view which repeat continually. The "tour" can be interrupted at any time for manual viewing. Inside cameras should be color with high resolution, low light capability, and discreet mounting, which means that they are not mounted on wall brackets making it easy to ascertain where they are being aimed.

4 .In non public areas, cameras should be fixed and aimed such that they cover approaching walkways, halls, and stairwells. Cameras mounted inside office areas are to provided on a case by case basis. Not all offices are considered high priority. Duress switches and motion detectors can provide alarm notification as well.

5. All camera images should be processed through motion detection equipment and interfaced into the main video matrix switching equipment so as to be called up when "activated" and viewed directly by the officer.

6. All cameras associated with any other detection devices such as door switches, motion detectors, etc. should also be interfaced to the video switching equipment to be called up to the main viewing monitor.

7. All exterior doors, including entrances to electrical and mechanical rooms, are to be monitored with door contact indicator switches. These switches are to be frame mounted with concealed wiring.

8. All areas on the first or ground level floors should have motion detectors where any outside access is possible. These motion detectors need to be armed and disarmed depending on the time and usage of the area.

9. High load detectors should be installed in all vehicle approaches to the campus and set to alarm for all large vehicles and or heavy loads entering the area. By interfacing this detection to the camera system, all large trucks could be visually monitored while on the premises. It would have been nice to know there was a Ryder truck parked outside the front door in Oklahoma City.

10. Vehicle detection loops should be installed at all delivery and service entrances, even when a gate or fence is present. This detection alarm will immediately draw attention of the security to this area, providing again a constant monitoring opportunity.

11. The use of metal and or X ray machines inside the building should be considered well based on the priority and perceived need the desired location. It is not recommended that these be directly visible to the public entering the building. However, at entrances to the House galleries and similar conference locations, it is not beyond the public's reasoning to be subjected to it. Everyone expects it at airports and should not object to it here. Whether or not the actual equipment is used, these locations should all have power and communication infrastructure installed to provide for the possible and clean usage of the equipment, if desired.

12. Provide a wireless duress system inside the building with adequate antenna coverage to envelope the entire interior area. This system should be interfaced with the security monitoring system to provide immediate location identification and the identity of the person in duress.

13. Emergency call station pedestals are to be located in parking and grounds areas with visibly marked signs. These locations need to also be "programmed" into the video system for immediate positioning when emergency calls are initiated.. The call stations only need to be equipped with audio and duress functions.